REMARKS

Claim Status:

Claims **1-27** are pending.

Claim Rejections - 35 USC 112

Claims **1-3, 13, 25** and **26**, and associated dependent claims (**2-8, 12-17, 21-23**), were rejected under 35 USC 112 as being indefinite. The Office states that the term "**random number**" is **indefinite** because the specification does not clearly redefine the term. Applicants respectfully **traverse**.

The Office asserts that the term "random number" *is used by the claim to mean a true "random number"*, while the accepted meaning is [a] *"pseudo-random number."* The Office cites a reference by Yolkowski supporting its assertion.

Nowhere does *Yolkowski* even mention the term *"pseudo-random number"*. Accordingly, the Office has not provided any **substantial, objective evidence** that the "accepted" meaning of the term "'random number" is "pseudo-random number." *See* In re Lee, 277 F.3d 1338 (Fed. Cir. 2002).

Nowhere in the instant Specification or Claims do the applicants act as his or her own lexicographer to define a specific or unusual meaning to the term "random number." **Nowhere** does the Specification state that the "random numbers" used in the methods taught therein **cannot** be "true" random numbers (such as might be generated by a radioactive decay process, or a quantum process, from hardware amplification of noise from a resistor or semiconductor in an electronic circuit). **Nowhere** does the Specification limit the term "random number" to be either a "true random number" or a "pseudo-random number." As such, the term "random number" must logically encompass both "true random number" and "pseudo-random numbers." It is improper, and unnecessary, therefore, for the Office to require that applicants amend the general term "random number" to be the more limited, restrictive term "pseudo-random number."

Applicants wish to draw the Examiner's attention to the reference by *Weisstein*, "Pseudorandom Number", shown in Appendix A. The citation for this reference is:

Eric W. Weisstein. "Pseudorandom Number." From *MathWorld*--A Wolfram Web Resource. *http://mathworld.wolfram.com/PseudorandomNumber.html.*

This web page was printed from the Internet on 05/03/2006. The source, Mathworld.Wolfram.Com, is a widely-used internet resource, described as follows:

"*MathWorld*TM is the web's most complete mathematical resource, assembled over more than a decade by internet encyclopedist Eric W. Weisstein with assistance from the mathematics and internet communities.

MathWorld is a comprehensive and interactive mathematics encyclopedia intended for students, educators, math enthusiasts, and researchers. Like the vibrant and constantly evolving discipline of mathematics, this site is continuously updated to include new material and incorporate new discoveries.

Although it is often difficult to find explanations for technical subjects that are both clear and accessible, this website bridges the gap by placing an interlinked framework of mathematical exposition and illustrative examples at the fingertips of every internet user."

Source: http://mathworld.wolfram.com/about/mathworld.html

MathWorld–A Wolfram Web Resource, is closely linked to Wolfram Research (see http://www.wolfram.com), which publishes the highly-regarded *Mathematica*™ research tool.

In the reference by *Weisstein* in Appendix A, he states that the term "Pseudorandom Number" is: *"A slightly **archaic** term for a computer-generated random number. The prefix pseudo- is used to distinguish this type of number from a "truly" random number generated by a random physical process such as radioactive decay."*

Weisstein teaches that the term "Pseudorandom Number" is an archaic (i.e., old, unused) term, and, as such, this **refutes** the Office's assertion that "Pseudorandom Number" is the "well-accepted" wording.

The Specification teaches, for example, on page , lines 12-14, that:

"The encryption key used is generated per message based on two pieces of information: ***a set of random numbers from a CD*** *(Compact Disk) and a token that is updated routinely."*

This set of random numbers, stored on a CD, could have been originally created from either a truly random physical process, such as radioactive decay; or from a pseudorandom number generator algorithm/program implemented on a computer. The Specification doesn't limit whether the **set of random numbers from a CD** are "true" random numbers or "pseudo-random" numbers; i.e., they could be either type. The methods disclosed and claimed in the present application for performing anonymous authenticated communications do not depend on which type of random number is stored on the CD; they could be either true" random numbers or "pseudo-random" numbers. The methods are independent of the two different "types".

A person of ordinary skill in the art of cryptography clearly understands that the term "random number" encompasses both "true random numbers" and "pseudo-random numbers." One can easily find sources on the Internet to purchase CD-ROMS containing lists of truly random numbers generated by, e.g., radioactive decay, or hardware noise.

Accordingly, the use of the term "random number" in claims **1-3, 13, 25** and **26**, and associated dependent claims is **definite** and **well-understood** by a person or ordinary skill in the art; and, as such, is not indefinite. Applicants respectfully request that the Office withdraw its rejections under 35 USC 112.

Claims 22 and 23

The Office rejected claims **22** and **23** as being indefinite under 35 USC 112, stating that the terms "**absolute**" and "**relative**" are not sufficiently well-defined by the specification. In response, claims **22** and **23** were amended to **delete** these terms, respectively. In addition, claim **23** was amended to additionally recite:

23. (currently amended) The method of claim 1, wherein the method provides ~~relative~~ anonymity for communications between the members by not providing for communications between members of the group within a same domain.

Support for this amendment to claim **23** can be found in the specification at page 7, lines 6-8.

Accordingly, claims **22** and **23** are now definite, and the rejections under 35 USC 112 have been overcome.

Claim Rejections - 35 USC 102(a)

Claims **1-8, 12-17, 21-23,** and **25-27** were rejected under 35 USC 102(a) as being anticipated by England et al., US Patent 6,327,652. Applicants respectfully **traverse**.

England et al. is **not a proper reference** that can be used against these claims. The present application claims priority benefit to an earlier Provisional Application Serial No. 60/311,733 filed August 9, 2001. (See Specification page 1, lines 6-8). Applicants respectfully submit that they conceived of the invention on at least as early as the Provisional's filing date (08/09/2001). On the other hand, *England's* patent issued as a 12/04/2001, which is after the date the Provisional application was filed. Since the applicants' invention occurred **before** the date of *England's* patent, the rejections under 35 USC 102(a) are improper and should be withdrawn.

Allowable Subject Matter

The Office indicated that claims **9-11, 18-20,** and **24** would be allowed if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicants gratefully acknowledge allowance of these claims.

Claim **9** was amended to be in independent form, including all of the limitations of the base claim **1**. Claims **10** and **11** depend from claim **9**.

Claim **18** was amended to be in independent form, including all of the limitations of the base claim **1**, and dependent claim **17**. Claims **19** and **20** depend from claim **18**.

Claim **24** was amended to be in independent form, including all of the limitations of the base claim **1**, and dependent claim **23**.

Accordingly, claims **9-11, 18-20,** and **24** are now in condition for allowance.

CONCLUSION

Applicants have responded to each and every objection and rejection, and urge that claims **1-27** as presented and amended are now in condition for allowance. Applicants request expeditious processing to issuance.

The Office is authorized to charge **Deposit Account # 19-0131** for any necessary fees regarding this response, including any extensions of time for reply, and for any additional independent claims.

Respectfully submitted,

Robert D. Watson

Robert D. Watson
Reg. No. 45,604

Ph: (505) 845-3139
Fax: (505) 845-2391

e-mail: rdwatso@sandia.gov

Sandia National Laboratories
P.O. Box 5800 MS-0161
Albuquerque, NM 87185-0161

Customer No. **20567**

Certificate of Transmission under 37 CFR 1.10

I hereby certify that this correspondence was transmitted via facsimile to the U.S. Patent and Trademark Office at phone number **571-273-8300** on **May 3, 2006.**

Robert D. Watson

Robert D. Watson

APPENDIX A

Pseudorandom Number

COMMENT
On this Page

A slightly archaic term for a computer-generated random number. The prefix pseudo- is used to distinguish this type of number from a "truly" random number generated by a random physical process such as radioactive decay.

SEE ALSO: Quasirandom Sequence, Random Number. [Pages Linking Here]

REFERENCES:

Luby, M. *Pseudorandomness and Cryptographic Applications*. Princeton, NJ: Princeton University Press, 1996.

Press, W. H.; Flannery, B. P.; Teukolsky, S. A.; and Vetterling, W. T. *Numerical Recipes in FORTRAN: The Art of Scientific Computing, 2nd ed.* Cambridge, England: Cambridge University Press, p. 266, 1992.

CITE THIS AS:

Eric W. Weisstein. "Pseudorandom Number." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/PseudorandomNumber.html